



# UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE  
United States Patent and Trademark Office  
Address: COMMISSIONER FOR PATENTS  
P.O. Box 1450  
Alexandria, Virginia 22313-1450  
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/785,535	02/16/2001	Norman H. Margolus	11656-002001	5190

26161 7590 06/23/2003

FISH & RICHARDSON PC  
225 FRANKLIN ST  
BOSTON, MA 02110

EXAMINER

PHAM, HUNG Q

ART UNIT	PAPER NUMBER
----------	--------------

2172

DATE MAILED: 06/23/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

**Office Action Summary**

Application No.

09/785,535

Applicant(s)

MARGOLUS ET AL.

Examiner

HUNG Q PHAM

Art Unit

2172

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

**Period for Reply**

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

**Status**

- 1) ☒ Responsive to communication(s) filed on 09 May 2003.
- 2a) ☐ This action is **FINAL**.                      2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

**Disposition of Claims** 1-153

- 4) ☒ Claim(s) ~~1-97~~ is/are pending in the application.  
4a) Of the above claim(s) 98-153 is/are withdrawn from consideration.
- 5) ☐ Claim(s) \_\_\_\_\_ is/are allowed.
- 6) ☒ Claim(s) 1-97 is/are rejected.
- 7) ☐ Claim(s) \_\_\_\_\_ is/are objected to.
- 8) ☐ Claim(s) \_\_\_\_\_ are subject to restriction and/or election requirement.

**Application Papers**

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on \_\_\_\_\_ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.  
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
- 11) ☐ The proposed drawing correction filed on \_\_\_\_\_ is: a) ☐ approved b) ☐ disapproved by the Examiner.  
If approved, corrected drawings are required in reply to this Office action.
- 12) ☐ The oath or declaration is objected to by the Examiner.

**Priority under 35 U.S.C. §§ 119 and 120**

- 13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).  
a) ☐ All b) ☐ Some \* c) ☐ None of:  
1. ☐ Certified copies of the priority documents have been received.  
2. ☐ Certified copies of the priority documents have been received in Application No. \_\_\_\_\_.  
3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).  
\* See the attached detailed Office action for a list of the certified copies not received.
- 14) ☒ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).  
a) ☐ The translation of the foreign language provisional application has been received.
- 15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

**Attachment(s)**

- 1) ☒ Notice of References Cited (PTO-892)                      4) ☐ Interview Summary (PTO-413) Paper No(s). \_\_\_\_\_
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)                      5) ☐ Notice of Informal Patent Application (PTO-152)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449) Paper No(s) 6 & 7 .                      6) ☐ Other: \_\_\_\_\_

Art Unit: 2172

**DETAILED ACTION**

***Election/Restrictions***

1. Applicants' election without traverse of Group I (claims 1-97) in Paper No. 9 is acknowledged. The non-elected claims 98-153 are withdrawn from consideration.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

Art Unit: 2172

**DETAILED ACTION**

***Election/Restrictions***

1. Applicants' election without traverse of Group I (claims 1-97) in Paper No. 9 is acknowledged.

***Claim Rejections - 35 USC § 103***

2. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

(a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negated by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

**3. Claims 1-7, 9-17, 19, 54-56, and 60-61 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1].**

Regarding to claim 1, Wong teaches a method for storing image datasets received from a plurality of image acquisition computers, and displaying requested image datasets retrieved from the image archive server to a plurality of display stations. As shown in FIG. 3, in step 36, the image dataset  $I_d + I_h$  is received from the digital imaging source 14 and in step 38 the image data  $I_d$  is compressed if desired. The compressed image data, or the raw image data if no compression is denoted  $L$  and its length  $L_L$ . In step 40, the first  $n$  bytes of this possibly compressed image data  $L$  is encrypted to form the data  $N = E_K(n)$ , having a length  $L_N$ , where  $E$  is a secret key encryption function and  $K$  is the secret key (Col. 5, lines 1-28) as the step of *encrypting the data item using a key derived from the content of the data item*. In step 42, the image data is modified in a form suitable for archiving in PACS image data store 28. In steps 44, 46, and 48 a hash  $H$  as *digital fingerprint* is computed from the modified image data, an identifier  $ID$  is formed from pertinent portions of the identifying information extracted from the modified image header, and the hash/identifier pair are sent to the authentication server (Col. 5, lines 29-59, Col. 1, line 62-Col. 2, line 8) as the step of *determining a digital fingerprint of the data item*. Wong does not explicitly teach the step of *storing the data item on the storage device at a location or locations associated with the digital fingerprint*. However, Wong further discloses the image data is stored at image data store 28, and the hash is stored in the authentication data store 34 maintained by

Art Unit: 2172

authentication server 32, which is associated with image data store via data network 26 (Col. 6, lines 1-16, FIG. 1, Col. 3, line 35-Col. 4, line 16). Thus, this technique illustrates the step of *storing the data item on the storage device at a location or locations associated with the digital fingerprint*. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including the step of storing data at a location or location associated with the fingerprint in order to authenticate and secure the link(s) between the acquisition computers associated with the various imaging devices and the PACS archive server.

Regarding to claim 2, Wong teaches all the claimed subject matters as discussed in claim 1, Wong further discloses the step of *testing for whether a data item is already stored in the repository by comparing a digital fingerprint of the data item to digital fingerprints of data items already in storage in the repository* (Col. 4, lines 60-65).

Regarding to claim 3, Wong teaches all the claimed subject matters as discussed in claim 2, Wong further discloses the step of *the same digital fingerprint is used for storing the data item on the storage device and for testing whether a data item is already stored in the repository* (Col. 5, lines 49-59).

Regarding to claim 4, Wong teaches all the claimed subject matters as discussed in claim 1, Wong further discloses *the encrypting of the data item is performed by the client prior to transmitting the data item to the storage device* (FIG. 3).

Regarding to claim 5, Wong teaches all the claimed subject matters as discussed in claim 4, Wong further discloses the step of *encrypting the key and storing the encrypted key on the storage device or on another storage device connected to the network* (FIG. 1).

Regarding to claim 6, Wong teaches all the claimed subject matters as discussed in claim 5, Wong further discloses *a client or user specific key is used to encrypt the key derived from the content of the data item* (Col. 5, lines 1-28).

Regarding to claim 7, Wong teaches all the claimed subject matters as discussed in claim 1, Wong further discloses *the key derived from the content of the data item is the same for all instances of the data item stored in the repository* (Col. 5, lines 1-28).

Regarding to claim 9, Wong teaches all the claimed subject matters as discussed in claim 2, Wong further discloses *one or more additional copies or other forms of redundant information about the data items is stored on the storage device or on other storage devices connected to the network for data integrity, availability, or accessibility purposes and not to provide separate storage of the data item for different client programs* (FIG. 1).

Regarding to claim 10, Wong teaches all the claimed subject matters as discussed in claim 1, Wong further discloses the step of *associating the data item with*

Art Unit: 2172

*each of a plurality of access-authorization credentials, each of which is uniquely associated with a particular user or client program* (Col. 5, lines 49-59).

Regarding to claim 11, Wong teaches all the claimed subject matters as discussed in claim 2, Wong further discloses the step of *associating the data item with each of a plurality of access-authorization credentials, each of which is uniquely associated with a particular user or client program* (Col. 5, lines 49-59).

Regarding to claim 12, Wong teaches all the claimed subject matters as discussed in claim 10, Wong further discloses the step of *storing a plurality of named objects, each named object comprising information representative of the data item paired with information representative of one of the access-authorization credentials* (Col. 5, lines 49-59).

Regarding to claim 13, Wong teaches all the claimed subject matters as discussed in claim 12, Wong further discloses *the information representative of the data item is a digital fingerprint* (Col. 5, lines 49-59).

Regarding to claim 14, Wong teaches all the claimed subject matters as discussed in claim 12, Wong further discloses *the information representative of the access authorization credential is a cryptographic hash of all or part of the access-authorization credential* (Col. 5, lines 49-59).



Regarding to claim 15, Wong teaches all the claimed subject matters as discussed in claim 14, Wong further discloses *the cryptographic hash is an access identifier that uniquely identifies the data item for a particular user or client program* (FIG. 6, Col. 6, lines 23-35).

Regarding to claim 16, Wong teaches all the claimed subject matters as discussed in claim 12, Wong further discloses *the named object is a data structure created by the client program* (Col. 5, lines 49-59).

Regarding to claim 17, Wong teaches all the claimed subject matters as discussed in claim 12, Wong further discloses *the named object is a data structure created by a server program acting on behalf of the repository* (Col. 6, lines 10-21).

Regarding to claim 19, Wong teaches all the claimed subject matters as discussed in claim 12, Wong further discloses *a client retrieving a data item by accessing a named object using an access-authorization credential to select the named object, and using the contents of the named object to determine the location of the data item on the storage device* (Col. 4, lines 40-65, Col. 6, lines 22-64).

Regarding to claim 54, Wong teaches all the claimed subject matters as discussed in claim 12, Wong further discloses a data item is represented as a *composite*

*of data-items, and the component data-items are separately deposited in the repository (FIG. 1, Cols. 3-4).*

Regarding to claim 55, Wong teaches all the claimed subject matters as discussed in claim 54, Wong further discloses *lists of fingerprints for data-items making up a composite data-item are deposited as an index data item, which can be given an object-name and used for obtaining access to any of the component data-items* (Col. 6, lines 10-35).

Regarding to claim 56, Wong teaches all the claimed subject matters as discussed in claim 55, Wong further discloses *a proof-of-deposit is returned for each component deposit, and some or all of the proofs are presented when the index data item is given an object-name* (Col. 6, lines 10-35).

Regarding to claim 60, Wong teaches all the claimed subject matters as discussed in claim 15, Wong further discloses *the physical location at which information about named-objects is stored is based on access identifiers, to introduce reproducible pseudorandomness into the physical locations of the items* (Col. 6, lines 10-65).

Regarding to claim 61, Wong teaches all the claimed subject matters as discussed in claim 1, Wong further discloses *the fingerprints are determined from the data items, and this process produces randomly distributed numbers which can be used to*

*introduce reproducible pseudorandomness into the physical locations of the data items* (Col. 5, lines 29-59, Col. 1, line 62-Col. 2, line 8, Col. 6, lines 10-65).

**4. Claim 8 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Pond et al. [USP 4,864,616].**

Regarding to claim 8, Wong teaches all the claimed subject matters as discussed in claim 1, but fails to disclose *users of the method are grouped into families, and the key derived from the content of the data item is the same for all instances of the data item stored in the repository by users in the same family, but may be different for users in different families*. Pond teaches a method of cryptographically labeling electronically stored data and further discloses *users of the method are grouped into families, and the key derived from the content of the data item is the same for all instances of the data item stored in the repository by users in the same family, but may be different for users in different families* (Summary, Col. 2-4). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by grouping the users into families and using the same key for users in the same family as taught by Pond in order to control access to the image data.

**5. Claims 18, 20-30, 32-39, 47-48, 50-53, 57-58 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Whiting et al. [USP 5,778,395].**

Regarding to claim 18, Wong teaches all the claimed subject matters as discussed in claim 12, but fails to disclose *a client replacing an existing version of a named object with a new version of that named object, by replacing the existing association with a data item stored on the storage device with a new association*. Whiting teaches a method for backing up files, Whiting further discloses the differences between a file and its version in the previous backup may be computed so that only the changes to the file need to be written on the backup storage means (Whiting, Col. 5, lines 3-26). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including the step of replacing an existing version by replacing the association with a data item in order to back up file to a backup storage means.

Regarding to claim 20, Wong teaches all the claimed subject matters as discussed in claim 12, but fails to teach *the named objects further comprise version information associating different data items with different versions of the named object*. Whiting teaches a method for backing up files, Whiting further discloses *the named objects further comprise version information associating different data items with different versions of the named object* (Whiting, Col. 9, line 56-Col. 10, line 65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including the technique of version information in order to differentiate image datasets.

Regarding to claim 21, Wong and Whiting teaches all the claimed subject matters as discussed in claim 20, Whiting further discloses *a backup of data items stored on the storage device is accomplished by preserving copies of the current versions of named objects in existence at the time of the backup* (Whiting, Col. 7, line 59-Col. 8, line 20).

Regarding to claim 22, Wong teaches all the claimed subject matters as discussed in claim 1, but fails to teach *records are kept of the association between data items and names in order to define named objects, and wherein data items recorded as being associated with named objects are not: deleted from the repository, and wherein named objects are backed up by preserving copies of the named object records in existence at the time of the backup*. Whiting teaches a method for backing up files, Whiting further discloses *records are kept of the association between data items and names in order to define named objects, and wherein data items recorded as being associated with named objects are not deleted from the repository, and wherein named objects are backed up by preserving copies of the named object records in existence at the time of the backup* (Whiting, Col. 7, line 59-Col. 8, line 20). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by using the technique of defining named objects and preserving copies of the named objects in order to back up image datasets.

Art Unit: 2172

Regarding to claim 23, Wong and Whiting teaches all the claimed subject matters as discussed in claim 22, Whiting further discloses *a plurality of backups are made at spaced time intervals* (Whiting, Col. 1, lines 30-50).

Regarding to claim 24, Wong and Whiting teaches all the claimed subject matters as discussed in claim 22, Whiting further discloses *the backup is accomplished by declaring that after a prescribed moment in time a new version of each named object will be created the first time that a new data item is associated with it* (Whiting, Col. 7, line 59-Col. 8, line 20).

Regarding to claim 25, Wong and Whiting teaches all the claimed subject matters as discussed in claim 24, Whiting further discloses *the prescribed moment in time is determined separately for each named object* (Whiting, Col. 7, line 59-Col. 8, line 20).

Regarding to claim 26, Wong and Whiting teaches all the claimed subject matters as discussed in claim 22, Whiting further discloses *named objects are preserved by creating a new version of each named object each time that a new data item is associated with it* (Whiting, Col. 8, lines 21-40).

Regarding to claim 27, Wong and Whiting teaches all the claimed subject matters as discussed in claim 26, Whiting further discloses *versions of named objects that are deemed unnecessary are deleted* (Whiting, Col. 25, lines 9-39).

Regarding to claim 28, Wong and Whiting teaches all the claimed subject matters as discussed in claim 27, Whiting further discloses *the determination of which versions of a named object to delete is based in whole or in part on the times at which the versions were created, and the intervals between these times* (Whiting, Col. 25, lines 9-39).

Regarding to claim 29, Wong and Whiting teaches all the claimed subject matters as discussed in claim 20, Whiting further discloses the step of *preparing a digital time stamp of a plurality of named objects to allow a property of these named objects to be proven at a later date* (Whiting, Col. 12, lines 38-48).

Regarding to claim 30, Wong and Whiting teaches all the claimed subject matters as discussed in claim 29, Whiting further discloses *a random or other difficult to guess element is incorporated into the time stamp hash for each named object, to prevent the property from being proven if this element is deleted* (Whiting, Col. 28, line 35-Col. 29, line 9).

Regarding to claim 32, Wong teaches all the claimed subject matters as discussed in claim 12, but fails to disclose the step of *altering one or more properties or parameters associated with an access-authorization credential to change the access rights of a client or user to the data item referenced by that credential*. Whiting teaches a method for backing up files, Whiting further discloses the step of *altering one or more properties or*

Art Unit: 2172

*parameters associated with an access-authorization credential to change the access rights of a client or user to the data item referenced by that credential* (Whiting, Col. 7, lines 32-58).

Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including the step of altering one or more properties to change the access right in order to control access to the image dataset.

Regarding to claim 33, Wong teaches all the claimed subject matters as discussed in claim 2, but fails to disclose *a challenge step to ascertain that the client has the full data item*. Whiting teaches a method for backing up files, Whiting further discloses *a challenge step to ascertain that the client has the full data item* (Whiting, Col. 35, lines 8-63). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including a challenge step as taught by Whiting in order to control access to image dataset.

Regarding to claim 34, Wong and Whiting teaches all the claimed subject matters as discussed in claim 33, Whiting further discloses the step of *requiring that the client attempting to store a data item provide correct answers to inquiries as to the content of portions of the data item, or inquiries that require knowledge of this content* (Whiting, Col. 35, line 64-Col. 36, line 4).



Regarding to claim 35, Wong and Whiting teaches all the claimed subject matters as discussed in claim 34, Whiting further discloses *the data item content on which the challenge is based is selected with a degree of randomness* (Whiting, Col. 35, line 64-Col. 36, line 4).

Regarding to claim 36, Wong teaches all the claimed subject matters as discussed in claim 2, but fails to disclose *depositors use the client to stored data items in the repository, and at least some depositors are required to provide identification*. Whiting teaches a method for backing up files, Whiting further discloses *depositors use the client to stored data items in the repository, and at least some depositors are required to provide identification* (Whiting, Col. 35, lines 7-43). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including the requiring identification of depositors to store data items in order to control access to image dataset.

Regarding to claim 37, Wong and Whiting teaches all the claimed subject matters as discussed in claim 36, Whiting further discloses *rules for when a depositor must provide identification are selected in order to discourage unlawful distribution of access to the data item* (Whiting, Col. 35, lines 7-43).

Regarding to claim 38, Wong and Whiting teaches all the claimed subject matters as discussed in claim 37, Whiting further discloses *there is a greater degree of user*

Art Unit: 2172

*identification or a higher likelihood that user identification will be required when the data item being stored by the depositor has been indicated to be shareable with other users* (Whiting, Col. 28, line 35-Col. 29, line 10).

Regarding to claim 39, Wong and Whiting teaches all the claimed subject matters as discussed in claim 37, Whiting further discloses *a class of data items the items may only be shared if the depositor has provided adequate identification* (Whiting, Col. 28, line 35-Col. 29, line 10).

Regarding to claim 47, Wong teaches all the claimed subject matters as discussed in claim 2, but fails to disclose: *the client has a directory structure for the data items, the data items are stored in the repository, and the directory structure is not evident to the repository maintainers*. Whiting teaches a method for backing up files, Whiting further discloses: *the client has a directory structure for the data items, the data items are stored in the repository, and the directory structure is not evident to the repository maintainers* (Whiting, Col. 4, lines 19-45). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including a directory structure for data items in order to back up image dataset.

Regarding to claim 48, Wong teaches all the claimed subject matters as discussed in claim 2, but fails to disclose *the client program using the repository is a mirroring program which determines which data items to deposit in the repository, and*

Art Unit: 2172

*wherein that determination is based at least in part on the result of a comparison of digital fingerprints establishing that certain data items are not in the repository.* Whiting teaches a method for backing up files, Whiting further discloses *the client program using the repository is a mirroring program which determines which data items to deposit in the repository, and wherein that determination is based at least in part on the result of a comparison of digital fingerprints establishing that certain data items are not in the repository* (Whiting, Col. 7, line 59-Col. 9, line 10). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by including the step of determining which data items to deposit in the repository based on at least in part on the result of a comparison in order to back up image dataset.

Regarding to claim 50, Wong and Whiting teaches all the claimed subject matters as discussed in claim 48, Whiting further discloses *the default for deciding what data items to mirror is to mirror all or substantially all data items* (Whiting, Col. 7, line 59-Col. 8, line 40).

Regarding to claim 51, Wong and Whiting teaches all the claimed subject matters as discussed in claim 48, Whiting further discloses the step of *making a determination of which data items need to be transmitted to the repository, and wherein that determination is based primarily on a comparison of digital fingerprints for data items at the client and data items in the repository* (Whiting, Col. 18, line 66-Col. 19, line 53).

Regarding to claim 52, Wong teaches all the claimed subject matters as discussed in claim 10, but fails to disclose *the access –authorization credential is determined in part by computing a hash involving elements of the pathname for a file on the client computer*. Whiting teaches a method for backing up files, Whiting further discloses *the access –authorization credential is determined in part by computing a hash involving elements of the pathname for a file on the client computer* (Whiting, Col. 15, line 58-Col. 16, line 17). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by using the technique of computing a hash involving the pathname in order to back up image dataset.

Regarding to claim 53, Wong and Whiting teaches all the claimed subject matters as discussed in claim 52, Whiting further discloses *the path name hash is made unique to a client by introducing a reproducible but randomly chosen element into it* (Whiting, Col. 15, lines 58-Col. 16, line 17).

Regarding to claim 57, Wong teaches all the claimed subject matters as discussed in claim 56, but fails to disclose *when transmitting a composite data-item, the client uses fingerprints to avoid retransmitting components following loss of communication*. Whiting teaches a method for backing up files, Whiting further discloses *when transmitting a composite data-item, the client uses fingerprints to avoid retransmitting components following loss of communication* (Whiting, Col. 5, lines 3-34). Therefore, it

Art Unit: 2172

would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by using fingerprint to avoid retransmitting in order to reduce the network bandwidth.

Regarding to claim 58, Wong and Whiting teaches all the claimed subject matters as discussed in claim 57, Wong further discloses *the index data-item is encrypted with a key that is only made available to the repository at the moment of access* (Wong, Col. 6, lines 10-64).

**6. Claim 31 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Garthwaite et al. [USP 6,415,302 B1].**

Regarding to claim 31, Wong teaches all the claimed subject matters as discussed in claim 12, but fails to disclose the step of *determining that a data item stored on the storage device is not referenced by any named object, and reusing the storage space used to store the unreferenced data item*. Garthmaite teaches a garbage collection method by *determining that a data item stored on the storage device is not referenced by any named object, and reusing the storage space used to store the unreferenced data item* (Garthmaite, Col. 5, line 14-Col. 6, line 8). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by using the garbage collection method as taught by Garthmaite in order to free unused memory.

7. Claims 40-42 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Whiting et al. [USP 5,778,395] and Ho [USP 6,148,342].

Regarding to claim 40, Wong and Whiting teaches all the claimed subject matters as discussed in claim 38, but fails to disclose *identity information about the depositor is made available to anyone able to access the data item, to discourage unlawful sharing*. Ho teaches a method for managing sensitive data and further discloses *identity information about the depositor is made available to anyone able to access the data item*. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong and Whiting method by including the step of disclosing the identity information to discourage unlawful sharing in order to prevent unauthorized access to image dataset.

Regarding to claim 41, Wong, Whiting, and Ho teaches all the claimed subject matters as discussed in claim 40, Whiting further discloses *the identity information is stored in an encrypted form that the depositor and users subsequently accessing the shared data item can both read* (Whiting, Col. 28, lines 36-65).

Regarding to claim 42, Wong, Whiting, and Ho teaches all the claimed subject matters as discussed in claim 41, Whiting further discloses *the repository is not able to decrypt the identity information about the depositor* (Whiting, Col. 29, lines 10-21).

**8. Claims 43-46 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Whiting et al. [USP 5,778,395] and Deo [USP 5,594,227].**

Regarding to claim 43, Wong and Whiting teaches all the claimed subject matters as discussed in claim 37, but fails to disclose *the identity of some users has not been well verified, but restrictions are placed on sharing of data item deposited by such poorly verified users*. Deo teaches a method for protecting against unauthorized access of data contents by denying access to data contents on a smart card (Deo, FIG. 7) as the *identity of some users has not been well verified, but restrictions are placed on sharing of data item deposited by such poorly verified users*. Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong and Whiting method by using the technique of placing restriction on data deposited by poorly verified users in order to control access to image dataset.

Regarding to claim 44, Wong, Whiting and Deo teaches all the claimed subject matters as discussed in claim 43, Deo further discloses the step of *limiting access to data items deposited by a poorly verified user* (Deo, FIG. 7).

Regarding to claim 45, Wong, Whiting and Deo teaches all the claimed subject matters as discussed in claim 44, Deo further discloses *the limited access is provided by limiting the aggregate bandwidth provided for such accesses* (Deo, FIG. 7).

Regarding to claim 46, Wong, Whiting and Deo teaches all the claimed subject matters as discussed in claim 44, Deo further discloses *the limited access is provided by limiting the number of simultaneous accesses to the data items* (Deo, FIG. 7).

**9. Claim 49 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Whiting et al. [USP 5,778,395] and Dobbek [USP 6,308,325 B1].**

Regarding to claim 49, Wong and Whiting teaches all the claimed subject matters as discussed in claim 48, but fails to disclose *mirroring software is downloaded to the client using a bootstrap process, wherein a small bootstrap program is downloaded and executed, and the bootstrap program manages download and installation of the remainder of the mirroring software*. Dobbek teaches a method for downloading data, Dobbek further discloses *software is downloaded to the client using a bootstrap process, wherein a small bootstrap program is downloaded and executed, and the bootstrap program manages download and installation of the remainder of the mirroring software* (Dobbek, Col. 5, line 60-Col. 6, line 40, and Col. 2, lines 23-43). Therefore, it would have been obvious for



one of ordinary skill in the art at the time the invention was made to modify the Wong and Whiting method by downloading a bootstrap process for managing downloading and installing the software in order to have a software to control back up image dataset.

**10. Claim 59 is rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Kuzma [USP 5,781,901].**

Regarding to claim 59, Wong teaches all the claimed subject matters as discussed in claim 55, but fails to disclose *an email message is broken up into component items in such a manner that the individual attachments are separate component data-items*. Kuzma teaches a method for transmitting email attachments form a sender to a receiver of a network. Kuzma further discloses *the email message is broken up into component items in such a manner that the individual attachments are separate component data-items* (Kuzma, Col. 4, line 65-Col. 5, line 65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by using the technique of breaking an email into component items based on attachment in order to secure the message.

**11. Claims 62-63, 65 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Thomlinson et al. [USP 6,532,542 B1].**

Regarding to claim 62, Wong teaches all the claimed subject matters as discussed in claim 2, Wong fails to disclose *an access identifier is formed to provide proof of ownership of the data item stored in the repository, the access identifier is formed by producing a one-way hash including item-identifying information chosen by the client program to identify the data item, and the one-way hash cannot be reversed to permit the repository to discover the identity of the client program or user*. Thomlinson teaches a method to provide central storage for data items. Thomlinson further discloses *an access identifier is formed to provide proof of ownership of the data item stored in the repository, the access identifier is formed by producing a one-way hash including item-identifying information chosen by the client program to identify the data item, and the one-way hash cannot be reversed to permit the repository to discover the identity of the client program or user* (Thomlinson, Col. 10, line 43-Col. Col. 11, line 32 and Col. 7, lines 45-67). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong method by using a one-way hash to produce password as access identifier in order to control access to image dataset.

Regarding to claim 63, Wong and Thomlinson teaches all the claimed subject matters as discussed in claim 62, Thomlinson further discloses *the item-identifying information is associated with the data item on the client* (Thomlinson, FIG. 3).

Regarding to claim 65, Wong and Thomlinson teaches all the claimed subject matters as discussed in claim 62, Thomlinson further discloses *user-identifying*

*information is provided to the repository as part of the access-authorization credential*  
(Thomlinson, FIG. 3).

**12. Claims 64, 66-67 are rejected under 35 U.S.C. 103(a) as being unpatentable over Wong et al. [USP 6,557,102 B1] in view of Thomlinson et al. [USP 6,532,542 B1] and Whiting et al. [USP 5,778,395].**

Regarding to claim 64, Wong and Thomlinson teaches all the claimed subject matters as discussed in claim 63, but fails to disclose *the item-identifying information is derived at least in part from the path name of the data item on the client*. Whiting teaches a method for backing up files, Whiting further discloses the *item-identifying information is derived at least in part from the path name of the data item on the client* (Whiting, Col. 15, line 58-Col. 16, line 17). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong and Thomlinson method by using the technique of computing a hash involving the pathname in order to back up image dataset.

Regarding to claim 66, Wong and Thomlinson teaches all the claimed subject matters as discussed in claim 62, but fails to disclose *at least some access-authorization credentials can be transferred between users without the use of the repository*. Whiting teaches a method for backing up files, Whiting further discloses *at least some access-authorization credentials can be transferred between users without the use of the*

*repository* (Whiting, Col. 28, lines 35-65). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong and Thomlinson method by using the technique of transferring access-authorization credentials as taught by Whiting in order to back up image dataset in a share file server.

Regarding to claim 67, Wong and Thomlinson teaches all the claimed subject matters as discussed in claim 65, but fails to disclose *at least one class of users is not permitted to transfer access using access-authorization credentials*. Whiting teaches a method for backing up files, Whiting further discloses *at least one class of users is not permitted to transfer access using access-authorization credentials* (Whiting, Col. 29, lines 1-9). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Wong and Thomlinson method restricting one class of users for transferring access as taught by Whiting in order to protect the privacy of the image dataset.

**13. Claims 68, 70-82, 85-87, 89-97 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. [USP 5,778,395].**

Regarding to claim 68, Whiting teaches a method for backing up files from disk volumes on multiple nodes of a computer network to a common random-access backup storage means. In order to back up files from multiple nodes, a fingerprint is computed over fixed-size portions of the file contents as the step of *determining a digital fingerprint*

Art Unit: 2172

*of the data item* (Col. 18, lines 36-65). Whiting further discloses, to back up a new or updated file, a 32-bit hash over the relevant directory entry information is used for comparison instead of the full directory entry, and a complete hash value over the file contents is compared, as well as the least significant 16-bits of the file size. If all of these values match, the file being backed up is considered to be a match to the file in the database, resulting in a false match probability (Col. 20, line 42-Col. 21, line 18).

This technique indicates the step of *testing for whether the data item is already stored in the repository by comparing the digital fingerprint of the data item to the digital fingerprints of data items already in storage in the repository*. Whiting does not explicitly teach the step of *challenging a client that is attempting to deposit a data item already stored in the repository, to ascertain that the client has the full data item*. However, as taught by Whiting, a User Account Database contains the list of user names, user directory names, user ID values, as well as encryption and password keys for each user. Most of the record associated with each user in this file is encrypted using the user's private password. The data of each file in the backup set is stored in an encrypted form in the backup data file, where the encryption key is based on a fingerprint of the file's data itself. These "encryption" fingerprints themselves are then stored in a section of the backup directory file, which is itself encrypted with a key that is accessible to the user only by supplying a password (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65). As shown in FIG. 1, the nodes to be backed up may be workstations 102, desktop personal computers 103, laptop computers 104, or other servers 105 on the network. As shown in FIG. 2, each node is assigned two directories, a user directory and a system directory, on the backup

Art Unit: 2172

storage means 101. The node has network write access to its user directory, where it posts backup data (Col. 7, lines 8-58). Thus, when a node backups or updates its files into the backup storage, the combination of password and fingerprint as a challenge to inquiry a file for detecting a match before writing a new file, or updating an exist file as discussed above indicates the step of *challenging a client that is attempting to deposit a data item already stored in the repository, to ascertain that the client has the full data item.*

Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Whiting method by including the step of challenging a client to ascertain the client has the full data item in order to backup a file into the backup storage.

Regarding to claim 70, Whiting teaches all the claimed subject matters as discussed in claim 68, Whiting further discloses the step of *requiring that the client provide correct answers to inquiries as to the content of portions of the data item, or inquiries that require knowledge of this content* (Whiting, Col. 35, line 64-Col. 36, line 4).

Regarding to claim 71, Whiting teaches all the claimed subject matters as discussed in claim 70, Whiting further discloses *the challenge is based is not easily predicted by the user or client program* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 72, Whiting teaches all the claimed subject matters as discussed in claim 70, Whiting further discloses *the data item content on which the challenge is based can be determined by the client program without the aid of the repository* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 73, Whiting teaches all the claimed subject matters as discussed in claim 68, Whiting further discloses *future access to the data item deposited is provided by creating an access-authorization credential which can be presented at a later time to prove that the challenge has been met for that data item* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 74, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *each access authorization credential is uniquely associated with a access owner* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 75, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *each access authorization credential includes information sufficient to identify the access owner* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 76, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *the access authorization credential includes a fingerprint* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 77, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *the access authorization credential is associated with a fingerprint in the repository* (Col. 26, line 66-Col. 27, line 6; Col. 28, lines 35-65; Col. 20, line 42-Col. 21, line 18).

Regarding to claim 78, Whiting teaches all the claimed subject matters as discussed in claim 76, Whiting further discloses *the fingerprint is different from the fingerprint used for testing whether the data item is already stored in the repository* (Col. 20, line 42-Col. 21, line 18).

Regarding to claim 79, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *the access authorization credential is associated directly with the data-item or with a record in the repository that is associated with the data-item* (Col. 20, line 42-Col. 21, line 18).

Regarding to claim 80, Whiting teaches all the claimed subject matters as discussed in claim 79, Whiting further discloses *the record in the repository with which the*



Art Unit: 2172

*access authorization credential is associated is an access identifier that is associated with the credential by computation of a one way hash function* (Col. 18, line 36-Col. 19, line 53).

Regarding to claim 81, Whiting teaches all the claimed subject matters as discussed in claim 80, Whiting further discloses *the access identifier is stored in the repository and is compared with a later hash of an access authorization credential to verify access permission to a named object* (Col. 20, line 42-Col. 21, line 18).

Regarding to claim 82, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *the access authorization credential may include information sufficient to respond to a challenge* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 85, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting further discloses *at least some access-authorization credentials can be transferred between users without the aid of the repository* (Col. 28, lines 35-65).

Regarding to claim 86, Whiting teaches all the claimed subject matters as discussed in claim 85, Whiting further discloses *at least some access-authorization credentials is restricted for at least one class of access owner* (Col. 29, lines 1-9).

Art Unit: 2172

Regarding to claim 87, Whiting teaches all the claimed subject matters as discussed in claim 86, Whiting further discloses *the access authorization credential is only usable by the access owner* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 89, Whiting teaches all the claimed subject matters as discussed in claim 68, Whiting further discloses *at the time of deposit at least some data items are associated with a minimum expiration time* (Col. 7, line 59-Col. 8, line 20).

Regarding to claim 90, Whiting teaches all the claimed subject matters as discussed in claim 89, Whiting further discloses *at least some data items that expire are removed and their storage space reused* (Col. 25, lines 9-39).

Regarding to claim 91, Whiting teaches all the claimed subject matters as discussed in claim 90, Whiting further discloses *the repository keeps track of which access owners have deposited a given data item* (FIG. 2, Col. 7, lines 32-58).

Regarding to claim 92, Whiting teaches all the claimed subject matters as discussed in claim 91, Whiting further discloses *upon an access owner informing the repository that a data item is no longer needed, the data item is deleted or the expiration of the data item is accelerated* (Col. 7, line 59-Col. 8, line 20, Col. 25, lines 9-39).

Regarding to claim 93, Whiting teaches all the claimed subject matters as discussed in claim 92, Whiting further discloses *the repository truncates the list of depositors associated with a data-item, and never accelerates the expiration of this data item* (Col. 7, line 59-Col. 8, line 20; Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 94, Whiting teaches all the claimed subject matters as discussed in claim 68, Whiting further discloses the step of *encrypting the data item using a key derived from the content of the data item* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

Regarding to claim 95, Whiting teaches all the claimed subject matters as discussed in claim 94, Whiting further discloses *the encrypting of the data items is performed by the client prior to transmitting the data item to the storage device* (Col. 7, line 59-Col. 8, line 20).

Regarding to claim 96, Whiting teaches all the claimed subject matters as discussed in claim 94, Whiting further discloses the step of *encrypting the key and storing the encrypted key on the storage device or on another storage device connected to the network* (Col. 12, line 38-Col. 13, line 4).

Regarding to claim 97, Whiting teaches all the claimed subject matters as discussed in claim 96, Whiting further discloses *a client or user specific key is used to*

Art Unit: 2172

*encrypt the key derived from the content of the data item* (Col. 26, line 66-Col. 27, line 6, and Col. 28, lines 35-65).

**14. Claims 69, 83-84 are rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. [USP 5,778,395] in view of Armangau et al. [USP 6,549,992 B1].**

Regarding to claim 69, Whiting teaches all the claimed subject matters as discussed in claim 68, but fails to disclose: *the repository gives the client a deposit receipt which allows the user to prove that the deposit occurred*. Armangau teaches a method of backing up data from primary storage to tape; Armangau further discloses *the repository gives the client a deposit receipt which allows the user to prove that the deposit occurred* (Armangau, Col. 17, lines 6-28). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Whiting method by using the step of giving the receipt of backup data as taught by Armangau in order to confirm the transfer of backup data from a node to the backup storage.

Regarding to claim 83, Whiting teaches all the claimed subject matters as discussed in claim 73, Whiting fails to teach *data proof information created during a challenge process that is sufficient to prove to the repository that the challenge was passed*. Armangau teaches a method of backing up data from primary storage to tape; Armangau further discloses *data proof information created during a challenge process that*

Art Unit: 2172

*is sufficient to prove to the repository that the challenge was passed* (Armangau, Col. 17, lines 6-28). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Whiting method by using the step of giving the receipt of backup data as taught by Armangau in order to confirm the transfer of backup data from a node to the backup storage.

Regarding to claim 84, Whiting and Armangau teaches all the claimed subject matters as discussed in claim 83, Armangau further discloses *the data proof information comprises the actual challenge response, so that it can be directly verified against the data-item* (Armangau, Col. 17, lines 6-28).

**15. Claim 88 is rejected under 35 U.S.C. 103(a) as being unpatentable over Whiting et al. [USP 5,778,395] in view of Midgley et al. [USP 6,526,418 B1].**

Regarding to claim 88, Whiting teaches all the claimed subject matters as discussed in claim 86, but fails to disclose *the aggregate bandwidth available to all users of the access authorization credential is limited*. Midgley teaches a method for continuous back up of data stored on a computer network, Midgley further discloses *the aggregate bandwidth available to all users of the access authorization credential is limited* (Midgley, Col. 5, lines 21-56). Therefore, it would have been obvious for one of ordinary skill in the art at the time the invention was made to modify the Whiting method by using the

Art Unit: 2172

technique of controlling the bandwidth as taught by Midgley in order to manage the bandwidth when back up data file to the backup storage.

***Conclusion***

16. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Hung Pham whose telephone number is 703-605 4242. The examiner can normally be reached on Monday-Friday, 7:00 Am - 3:30 Pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, VU, KIM YEN can be reached on 703-305 4393. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746 7239 for regular communications and 703-746 7238 for After Final communications. Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305 3900.

Examiner: Hung Pham  
June 13, 2003

  
**SHAHID AL ALAM**  
**PATENT EXAMINER**